Latin American Cybersecurity: a Fast-Growth Priority
Latin American Cybersecurity: a Fast-Growth Priority
Latin American Cybersecurity: a Fast-Growth Priority

Carlos Gonzalez Fillad,
Managing Director, Regional Head of Latin America, Global Liquidity and Cash Management, HSBC

Lance Kawaguchi,
Managing Director, Global Head – Corporates, Global Liquidity and Cash Management, HSBC

The recent cyber breach of five firms in Mexico and the USD15mn exploitation of their connections to the SPEI\(^1\) domestic payment system\(^2\) have placed a spotlight on Latin American cybersecurity. However, while the losses may have raised awareness in the region, there is still much work to be done by corporates and their treasuries to prevent this sort of breach becoming more commonplace. Lance Kawaguchi, Managing Director, Global Head, Corporates, Global Liquidity and Cash Management and Carlos Gonzalez Fillad, Regional Head, Mexico City and Latin America, Global Liquidity and Cash Management at HSBC, examine the current cybersecurity landscape in the region and explore some of the best practices for cyber risk mitigation.

The Cyber Landscape

Corporate awareness and activity

Even before recent events in Mexico, which followed similar breaches from around the globe, corporate treasurers were becoming increasingly concerned about cybersecurity issues. A report by Celent\(^3\) in November 2017 revealed that 82 per cent of treasurers cited cybersecurity as their number one concern. Yet despite this, corporate preparations appear less than comprehensive, as the report also revealed that globally:

- 70 per cent of organisations have not developed a cyber-incident response plan
- 46 per cent of organisations have not implemented or enhanced their phishing awareness training for employees in the past 12-24 months
- 43 per cent of organisations lacked board-level responsibility for the review and management of cyber risk
- 37 per cent of organisations have not yet estimated the financial impact of a cyber attack
- 34 per cent of organisations do not assess their suppliers or customers for cyber risk.

Based upon various conversations with HSBC clients in Latin America, it seem likely that these figures would probably also be regionally representative. However, the picture is extremely varied, with a small percentage of treasuries having a sophisticated cybersecurity approach, a larger group who are increasingly cyber-aware, but a majority where both awareness and activity are low.

In general, these groupings seem to reflect the corporate demographic, with the largest corporations typically being the most active, while the large number of smaller companies are less active. However, irrespective of size, companies that trade internationally seem to be more cyber-aware than purely domestic organisations.

At one end of the spectrum, companies may be taking minimal or no cybersecurity measures, but even where companies have put security processes in place, control gaps still exist. For example, treasury staff may lend each other security tokens, or access to vendor data may not be stringently controlled. There is therefore a need not only to raise cyber awareness but also to be discovering and implementing global best practice. In both cases, there is definitely an important role for banks to play in supporting clients. This has been very apparent from the strongly positive response of Latin American corporate treasuries to cybersecurity events and information sharing offered by HSBC.

---

\(^1\) Sistema de Pagos Electrónicos Interbancarios


\(^3\) “Combatting Treasury Fraud: External Forces Changing the Cybercrime and Cyberfraud Landscape”, Celent, November 2017
Government awareness and activity
The response of governments in the region to cybersecurity is almost as diverse as that of corporates. Mexico has been among the most active. Even before the recent attacks, Mexico’s central bank had set out rules relating to the SPEI system that required financial institutions to have emergency response protocols prepared that would be triggered in the event of a cyber attack. The central bank has also announced the formation of a dedicated cybersecurity unit that will design and issue information security guidelines to the country’s banks.

Elsewhere, the Argentine government has already started working on cyber initiatives, including a cyber-policy partnership with the US. Despite these initiatives, there is still room for improvement in other Latin American countries, with a recent World Economic Forum paper reporting that Latin America was particularly vulnerable to cyber attacks and that many countries in the region still lacked the capacity to respond to major cyber incidents. This is perhaps understandable, because until now the primary focus for much of the available government (and bank) resources in Latin America has been on inhibiting the laundering of physical cash by narcotics cartels.

This further underlines the value of being able to rely on the support of a banking partner that has made a substantive investment and commitment to cybersecurity and that is open to sharing its knowledge of global best practice. In addition, as more Latin American companies expand into new trade corridors, the geographic extent of these capabilities across trade corridors will become increasingly important. For example, if a Mexican company has a business unit in China and there is a cyber attack there, the company will value insight on the Chinese cyber situation that can be provided at the head office in Mexico, as well as elsewhere.

The value of data
Treasury’s control of cash makes it an obvious target for hackers. However, what is less commonly realised is that direct monetary loss may not actually be the biggest risk: treasury is also an extremely attractive target for the theft of financial and commercial data. The potential reputational and indirect financial losses from this could be far more severe than a straightforward cash theft.

The data stolen could be sold on for commercial advantage, such as in bidding for a contract where knowing a competitor’s key price points is a major advantage. However, in industries such as aviation, there is also real concern that stolen technical data could be used for exploits, such as hijacking an aircraft.

More generally, while the average Latin American citizen may not regard corporate cash loss through cyber theft as of particular concern to them, they are definitely becoming much more aware of the personal risks to them of corporate or government cyber data theft. The last few years have seen a steady trickle of security failures by store chains, credit reporting agencies and government bodies. While the exact extent of the damage depends upon the data stolen, in some cases individuals had their identity data completely compromised, rendering them exceptionally vulnerable to identity theft. These individuals are unlikely to trust these organisations again, but the most severe failings may also have fundamentally undermined the integrity of the cyber ecosystem and its methods of identity validation.

Interconnection risk
In the case of treasury, this data loss risk has become more acute in recent years as its role has changed. Twenty years ago treasuries were far more detached from the rest of the business (in terms of both technology and processes) than they are today. Treasuries typically now play a far more consultative role in the business, which coupled with the ubiquity of enterprise resource planning (ERP) systems makes them far more integrated with the rest of the business and thus a highly attractive target for the theft of both cash and data.

Greater technical connectivity and the rise of straight through processing have unfortunately also given hackers a new attack vector. When a client submits a payment file to their bank, the bank processes it automatically. Therefore, if attackers manage to hack a corporate ERP system they could alter payment files to send payments to bogus vendor bank accounts that they control. A similar risk applies to treasury management systems. In both cases, having access to process consulting that includes qualified local language in-country specialists in ERP and treasury management systems can help in identifying and rectifying potential vulnerabilities in existing systems. However, as a growing number of Latin American corporates transition from paper to electronic processes, these specialists can also be invaluable in supporting secure initial system setup.

A bank that is capable of offering this breadth and depth of expertise can also add value by helping a corporation to do its own due diligence on its trading partners. A corporate may be secure, but if its suppliers or customers (and their counterparties in turn) are not, then the corporate itself is also indirectly at risk. The good news here is that a bank that operates globally across all categories and sizes of client will have conducted its own due diligence on each of them. While this obviously doesn’t offer a strict guarantee, the extensive scope of this counterparty scrutiny offers a measure of comfort to companies conducting their own due diligence if they know their counterparties also bank with the same reputable bank as themselves.

5 https://www.state.gov/r/pa/prs/ps/2017/04/270496.htm
6 https://www.weforum.org/agenda/2018/03/this-is-the-biggest-threat-to-latin-america-s-digital-transformation/
7 https://blogs.scientificamerican.com/observations/the-equifax-hack-bad-for-them-worse-for-us/
The weakest link: people
Technology measures, such as ensuring all network devices have the latest patches applied or installing deception technology, are undoubtedly an important element in effective cybersecurity. However, the benefits of these can be (and often are) completely negated by the human element, so a more holistic approach is needed that also accommodates this. Individuals still persist in clicking on phishing links or committing similar security indiscretions, thus giving hackers their opportunity.

Hackers are well aware of this unfortunate tendency. While they can and do automate scanning for technological shortcomings (such as unpatched hardware), they increasingly realise that carefully crafting a credible looking email with poisoned links to an individual within a company is likely to prove a more rewarding attack vector. In many cases, rather than technology, people (or the business processes they are responsible for) can be the weakest cybersecurity link.

Verizon’s most recent annual Data Breach Investigations Report analysed 53,000 actual cyber incidents, which included 2,216 confirmed data breaches across 85 countries. One of the report’s key statistics was that 4 per cent of phishing campaign targets would click a phishing link. Furthermore, this behaviour was persistent: someone who clicked a link once was more likely to do so again in the future.

One of the biggest challenges here is changing corporate culture. While individuals will take a measure of personal responsibility for physical risk in their organisation (such as sounding a fire alarm upon discovering a fire) this behaviour often doesn’t apply to cyber risks. Instead, the mindset seems to be: ‘the organisation takes care of all that, I don’t need to do anything’. Nothing could be further than the truth. Individuals have a personal responsibility at many levels, especially since the personalisation of attacks makes it easier for cyber criminals to succeed. Private indiscretions on social media today will boost the effectiveness of socially-engineered spear phishing attacks tomorrow.

This indifferent attitude of many individuals to their personal cyber responsibilities is alarming given that cyber crime continues to increase at a meteoric rate (partly because of the attractive risk/reward ratio for perpetrators when compared to physical crime). Just one example of this cyber crime growth in Latin America comes from statistics on Brazil in the AWPG’s most recent quarterly report, which included:

- A 379 per cent increase in phishing (430 in Q3 versus 1,631 in Q4)
- A 245 per cent increase in scam Web sites (2,562 in Q3 versus 6,293 in Q4)
- A 247 per cent increase in social media-based scams (1,909 in Q3 versus 4,724 in Q4).

Effective cyber training
Security awareness training, phishing tests, plus changing the corporate culture, are all valid steps in protecting against these threats, but a key point here is repetition. Organisations such as the InfoSec Institute recommend that best practice is to repeat security awareness training every 90 days. However, repetition will only be really effective if personnel also understand the reasoning behind the security processes they learn about during cyber training. Personnel circumventing secure measures in the interests of convenience is a common problem, but one that is less likely to occur if they understand the purpose and value of such measures.

While there are many generic good practices, training also needs to contain an element of role-specific material. For example, a software developer who never leaves the office faces different threats from a sales person who often works from home. Cyber fraud attempts will also often be role-specific, such as treasury or finance personnel receiving bogus payment instructions seemingly from senior management via a faked email address. These types of attack have unfortunately been successful in the past, but the training required to prevent them is not especially onerous.

Alongside training, there is the need for internal measures to prevent corrupt employees from deliberately initiating or assisting cyber crime. Rigorous employee vetting can help, but also needs to be supported by other measures, such as whistle blowing policies and technological solutions.

Another key point is the sharing of best practice and expertise, both internally and externally. For example, due to the nature of their role, treasuries have a strong control background and can add value by sharing that mindset with other functions that do not.

The global nature of cyber threats also needs to be incorporated into corporate security strategy and training. Companies with overseas subsidiaries face a particular challenge here, but the value of rapid information exchange is equally applicable to purely domestic entities. A new and successful type of attack in one country is likely to be reused elsewhere around the globe shortly thereafter. In some recent attacks, such as Petya, the speed of spread both within corporations and globally has been extremely rapid: on one global corporate’s network, 62,000 servers and workstations were knocked offline by Petya within an hour. A global banking partner can be indispensable in a situation like this if it is able to aggregate the cybersecurity information it collects across its entire network in real time and can share it with clients wherever they require.

---

9 https://resources.infosecinstitute.com/security-awareness-course-design-best-practices/#ref
Investing in business continuity

Though the statistics in the Celent report on the lack of board-level responsibility for cybersecurity are hardly encouraging, there are signs that this attitude is changing. From client conversations it appears that more boards are now accepting cyber responsibility and more treasuries are allocating budgets for cybersecurity, both within treasury as well as in the business more generally.

A robust strategy coupled with investment in both technological and personnel cybersecurity measures can do much to make a corporation relatively unattractive for targeted attacks and less vulnerable to generic attacks. However, it is unsafe to assume that even the most stringent measures will guarantee invulnerability, so having a business continuity plan (BCP) that incorporates cyber as well as physical threats is essential. This needs to include measures that will enable the business to function (even if only at a basic level) while the clean up takes place. (It may also include sharing information on the attack with trusted partners so that they can share information anonymously with other parties to hinder further external propagation of the attack.)

In the event of a serious attack, it is possible that the company’s usual processes for making payments will be out of action. For instance, HSBC has see at least one example of a Latin American client whose ERP was the subject of a ransomware attack, leaving it unable to pay staff salaries and suppliers. HSBC assisted by scanning its own systems to retrieve details of previous transactions and payee details. Then using a highly secure manual payment process provided by HSBC, the client was at least able to make the majority of the necessary payments.

In this example, HSBC provided the workaround on an ad hoc basis, but having a back up process of this nature in place as part of a cyber BCP makes sense. However, accomplishing this requires the support of a bank that has a deep understanding of how the business functions and the nature of its financial flows and can leverage that on the client’s behalf in a cyber crisis.

For many Latin American companies, the priority in recent years has been growth, so their focus has typically not been on developing a cyber BCP, even though they may already have a BCP for physical risks. Partly driven by recent cyber events, this attitude is gradually starting to change. In some cases they are beginning to appreciate that growth through acquisition may require a separate cyber BCP in its own right. A company’s existing measures, processes and personnel may be relatively secure, but what about those of an acquisition it makes? These need to be evaluated, ideally by expert process consultants who can identify any weaknesses in processes and technology, and recommend appropriate remedies. An acquisition may need to be an additional element in a cyber BCP that will require updating as the acquisition is on-boarded and its systems and processes transition to those of the acquirer.
Conclusion

Latin American companies and their treasuries are increasingly keen to learn more about cybersecurity best practice and how to implement it. However, an important factor in achieving this is to understand that this is an ongoing process (not a ‘fit and forget’) – as is any investment required to support it. It is therefore not unreasonable for these companies to expect a similar (or greater) level of cyber commitment from their banks. It is not just that corporates understandably need to feel that their banks are following best cyber practice in handling client data and payments, but that they are also leading it and sharing it globally. This could cover a broad spectrum, ranging from news of attacks and possible mitigation methods, to the development of new authentication methods such as biometrics. Having access to this sort of expertise as part of a close working relationship can add significant value for a corporate trying to develop, implement or extend a cybersecurity strategy.